1 Билет №9. Нечилловая формулка для символа Лежандра

1.1 Лемма

Пусть $p \in \mathbb{P},\ p_1 = \frac{p-1}{2},\ a \in \mathbb{Z},\ a \not\vdots\, p$. Тогда

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{2ax}{p}\right]}$$

1.2 Доказательство

Пусть $\varepsilon_i \in \{-1; 1\},\ r_i \in [-p_1, p_1]$.

$$a \cdot 1 \equiv_p \varepsilon_1 r_1$$

$$a \cdot 2 \equiv_p \varepsilon_2 r_2$$

$$\dots$$

$$a \cdot p_1 \equiv_p \varepsilon_{p_1} r_{p_1}$$

Числа $r_1, \dots, r_{p_1}$ являются разными вычетами по модулю p. Числа $1, \dots, p_1$ также являются разными вычетами по модулю p. Отсюда следует, что перемножение $r_1, \dots, r_{p_1}$ будет сравнимо с перемножением $1, \dots, p_1$ по модулю p (одно будет являться перестановкой другого).

Предположим, что $r_i \equiv_p r_j$. Тогда

$$ax_i \equiv_p ax_j$$

$$ax_i - ax_j \equiv_p 0$$

$$a(x_i - x_j) \equiv_p 0$$

Но $(a, p) = 1$ и $x_i \neq x_j$. Противоречие.

Перемножем написанные равенства вида $ax \equiv_p \varepsilon_x r_x$.

$$a \equiv_p \varepsilon_1 \dots \varepsilon_{p_1}$$

Пусть вычет ax находится в промежутке от 1 до $\frac{p-1}{2}$, тогда $\varepsilon = 1$. Докажем это.

$$kp + 1 \leq ax \leq kp + \frac{p-1}{2}$$

$$2kp + 2 \leq 2ax \leq (2k+1)p - 1$$

$$2k + \frac{2}{p} \leq \frac{2ax}{p} \leq 2k + \frac{p-1}{p}$$

Отсюда следует, что целая часть $\left[\frac{2ax}{p}\right] = 2k$, так как $\frac{2}{p} < 1,\ \frac{p-1}{p} < 1$.

Аналогично докажем, что $\varepsilon = -1$, когда $ax \in \left[kp + \frac{p-1}{2} + 1; (k+1)p - 1)\right]$.

$$kp + \frac{p-1}{2} + 1 \leq ax \leq (k+1)p - 1)$$

$$(2k+1)p + 1 \leq 2ax \leq (2k+2)p - 2$$

$$2k + 1 + \frac{1}{p} \leq \frac{2ax}{p} \leq 2k + 2 - \frac{2}{p}$$

$$2k + 1 + \frac{1}{p} \leq \frac{2ax}{p} \leq 2k + 1 + \frac{p-2}{p}$$

$$\left[\frac{2ax}{p}\right] = 2k + 1$$

Основываясь на двух предыдущих доказательствах, можем сказать, что

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]}$$

Следовательно,

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}} \equiv_p a^{p_1} \equiv_p \varepsilon_1 \dots \varepsilon_{p_1} \equiv_p (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{2ax}{p}\right]}$$

2 Билет №10. Очень страшные формулы

2.1 Лемма

Пусть $p \in \mathbb{P}$ и $p_1 = \frac{p-1}{2}$.

1. (Второе дополнение к закону взаимности Гаусса)
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

2. Пусть $a \in \mathbb{Z},\ a \not\vdots\, p,\ a \not\vdots\, 2$. Тогда
$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]}$$

2.2 Доказательство

$$\left(\frac{2a}{p}\right) \equiv_p \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) \equiv_p \left(\frac{\frac{a+p}{2}}{p}\right) \equiv_p (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]} \equiv_p (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}+x\right]} \equiv_p (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\sum\limits_{x=1}^{p_1} x} \equiv_p (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{(p_1+1)p_1}{2}}$$

$$\left(\frac{2a}{p}\right) \equiv_p (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}}$$

Подставим $a = 1$. Так как $x \le \frac{p-1}{2}$, то $\frac{ax}{p} = \frac{2x}{p} < 1$. Значит, $\left[\frac{2x}{p}\right] = 0$ и $\sum\limits_{x=1}^{p_1}\left[\frac{2x}{p}\right] = 0$.

$$\left(\frac{2}{p}\right) \equiv_p (-1)^{\frac{p^2-1}{8}}$$

$$\left(\frac{2a}{p}\right) \equiv_p \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) \equiv_p (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}}$$

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]}$$

3 Билет №11. Закон взаимности Гаусса

3.1 Теорема

Пусть $p, q \in \mathbb{P}$ нечётны. Тогда
$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

3.2 Доказательство

Пусть $p_1 = \frac{p-1}{2},\ q_1 = \frac{q-1}{2}$.
$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum\limits_{y=1}^{q_1}\left[\frac{py}{q}\right]+\sum\limits_{x=1}^{p_1}\left[\frac{qx}{p}\right]}$$

Пусть p_1q_1 — количество пар $(x; y)$. p_1q_1 — это также количество пар $(qx; py)$.

$$qx \neq py$$

Предположим, что это не так. Тогда $qx = py$ и $qx \,\vdots\, p$, но p и q — взаимно простые, а $x < p$, поэтому $qx \not\vdots\, p$. Значит у нас существует какое-то количество пар S_1, где $qx < py$, и какое-то количество пар S_2, где $qx > py$. Отсюда следует, что $p_1q_1 = S_1 + S_2$. Найдём эти количества.

$$qx < py$$

$$x < \frac{py}{q}$$

Целых чисел, которых меньше, чем $\frac{py}{q}$, ровно $\left[\frac{py}{q}\right]$. И так как $y \in [1; q_1]$, то

$$S_1 = \sum_{y=1}^{q_1} \left[\frac{py}{q}\right]$$

Аналогично,

$$S_2 = \sum_{x=1}^{p_1} \left[\frac{qx}{p}\right]$$

Значит,

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{p_1 q_1} = (-1)^{S_1 + S_2} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$